DocuSign Envelope ID: 10489A29-B845-4741-AFAA-C34BB47D7AD0

Agreement for Disclosure of Unemployment Insurance Data and Information

I. Parties to the Agreement

This Agreement for Disclosure of Unemployment Insurance Data and Information is entered into by the Wisconsin Department of Workforce Development, Unemployment Insurance Division (DWD) and the Wisconsin Department of Justice (DOJ), Division of Criminal Investigation ("Data Recipient").

II. Scope and Purpose of this Agreement

A. This Agreement governs use and disclosure of all unemployment insurance data and information disclosed at any time by DWD to Data Recipient and in the possession or control of Data Recipient on or after the effective date of this Agreement (referred to in this Agreement as "UI Data"). This Agreement also establishes, in the Memorandum of Understanding attached to this Agreement, the relationship between DWD and the Data Recipient with respect to the Wisconsin ACISS Case Management System, and sets forth the respective obligations and commitments of each party with respect to ACISS. This Agreement shall control if there is an inconsistency between this Agreement and the ACISS Memorandum of Understanding attached to this Agreement.

B. The purposes of this Agreement are:

1. To comply with 20 CFR Part 603, Wis. Stat. § 108.14(7) and Wisconsin Administrative Code Chapter DWD 149 ("DWD 149"), which require DWD, in disclosing UI Data to certain persons and entities, to enter into an agreement with such persons and entities that contains certain required confidentiality safeguards, record disclosure requirements and consequences for breach.

2. To assure DWD that Data Recipient will comply with all of the applicable requirements of 20 CFR Part 603 and DWD 149 regarding the sharing of UI Data that occurs under this Agreement.

3. To specifically identify the UI Data that DWD will provide to Data Recipient under this agreement, the intended purposes for its use by Data Recipient, the limitations on such use and responsibility of Data Recipient for the costs and providing the UI Data to Data Recipient.

III. UI Data to Be Provided by DWD and Purposes for Its Use

A. DWD will provide to the DOJ Division of Criminal Investigation (DCI) UI Data of the type and under the conditions described as follows:

DCI will create and manage DOA mainframe accounts for its field office support staff and intelligence analysts at the Wisconsin Statewide Intelligence Center ("WSIC"). DWD will grant access for DCI field office support staff and WSIC intelligence analysts to Unemployment Insurance mainframe transactions screens

DocuSign Envelope ID: 10489A29-B845-4741-AFAA-C34BB47D7AD0

necessary to achieve the purpose stated in Section III.B of this agreement. The field office support staff and WSIC intelligence analysts will be able to obtain UI Data through this remote access system.

Certain UI Data are not accessible through the DWD's Unemployment Insurance mainframe transaction screens. In the event the field office support staff or WSIC intelligence analysts are unable to access UI Data necessary for the purpose stated in Section III.B of this agreement through the remote access system, the field office support staff or WSIC intelligence analysts will send an email to DWDUIRecordsCustodian@dwd.wisconsin.gov (**DWD MB UI Records Custodian** within the global address list) to request UI Data. The email will include a statement that this request is made in compliance with this DWD and DOJ's data sharing agreement and will identify the person whose UI Data is being requested by first name, last name, and the DOJ phone number DWD would call to obtain the Social Security number. The request will also detail the UI Data that is being requested, including the time period for which UI Data is needed, and that UI Data should be returned via email reply. Requests will be made on an as needed basis.

DWD will reply to the requestor via secure email to provide the requested UI Data. UI Data may include, but is not limited to, whether an individual applied for UI, whether the individual was found eligible for UI, whether the individual was paid UI, including dates and amounts of benefit payments, the date benefits were terminated, the individual's last known mailing address and phone number, employer's wage file and tax liability records, employer's account creation, correspondence, and payment records, and New Hire records.

DWD will also provide UI Data from worker classification investigations, from unemployment insurance fraud criminal investigation files, and potential criminal activity tips to DOJ via the ACISS Case Management system, a system owned by the DOJ and installed on their network. Attached to this Agreement is the Memorandum of Understanding regarding DWD's requirements for using the DOJ ACISS Case Management System. This Agreement details DOJ's requirements regarding the UI Data DWD will enter into ACISS.

B. Purpose for UI Data

The Data Recipient, a law enforcement agency of the State of Wisconsin, intends to use the UI Data disclosed under this Agreement solely for the following purposes:

The Data Recipient will use the UI Data as part of criminal investigations, including Suspicious Activity Reports and Terrorist Screening Center Watchlist inquiries. Records may be those of the criminal investigation subjects or may be for parties who are not the subject of the criminal investigation but whose records may provide leads or otherwise potentially forward the criminal investigation. DCI may use UI Data in the prosecution of criminal charges. DCI may also use the UI Data to verify information provided by, or to otherwise screen, applicants for employment with the DOJ.

DocuSign Envelope ID: 10489A29-B845-4741-AFAA-C34BB47D7AD0

DOJ's access and use of UI Data in the ACISS Case Management will be for the purpose of sharing the ACISS resource with DWD, for the purpose of criminal prosecution of unemployment fraud cases, and to provide Contact Pointer information to other ACISS users.

IV. Compensation for Costs of Providing UI Data

As long as Data Recipient provides DWD with access to ACISS Case Management, the costs incurred by DWD and Data Recipient are reciprocal and DWD will not charge Data Recipient for access to UI Data.

If Data Recipient ceases to provide DWD with access to ACISS Case Management, Data Recipient will compensate DWD for the actual, necessary and direct costs of location and disclosure of records and data. DWD will invoice Data Recipient for such costs. At its option, DWD may require payment of estimated costs in advance of incurring them and provide adjustments by subsequent credits or refunds.

V. Security and Confidentiality of UI Data

A. Data Recipient will utilize all procedures and security mechanisms necessary to prevent unauthorized access to or disclosure of the UI Data, including at a minimum the safeguards required by 20 CFR § 603.9 and DWD § 149.06 and specifically agrees that it will:

1. Use the UI Data only for purposes authorized by law and this Agreement.

2. Not disclose the UI Data without prior written approval of DWD and otherwise comply with the confidentiality requirements of DWD § 149.06, except as authorized in Section VI of this agreement.

3. Store the UI Data in a place physically secure from access by unauthorized persons.

4. Store and process the UI Data in an electronic format in a way that is secure from access by unauthorized persons.

5. Take precautions to ensure that only authorized personnel have access to the computer systems in which the UI Data is stored.

6. Make the UI Data accessible only to those staff of Data Recipient who require the data in the official performance of their job duties and for the specific purposes stated in this Agreement. All data will be kept in the strictest confidence and will be made available to staff of Data Recipient on a "need-to-know" basis.

7. Instruct all persons with access to the data on the confidentiality requirements of this Agreement, the applicable federal and state confidentiality requirements of 20 CFR § 603.9 and DWD § 149.06 and

DocuSign Envelope ID: 10489A29-B845-4741-AFAA-C34BB47D7AD0

the sanctions specified by law for unauthorized disclosure of information. If requested by DWD, Data Recipient will sign an acknowledgement that all persons with access to the information will be so instructed or have signed agreements to maintain security and confidentiality of UI Data.

8. Maintain a system sufficient to allow a complete and efficient audit of compliance with these safeguard provisions and the other requirements of this Agreement, including complete records of all use, disclosure and limitations on such use and disclosure of UI Data.

9. Provide access to DWD for on-site inspection in order to audit compliance and assure that the requirements of state and federal law and this Agreement are met.

10. Adhere to State of Wisconsin and DWD guidelines on data handling and security during the term of this Agreement and during any audit period thereafter.

11. Destroy the UI Data in a manner and at times specified in writing by DWD.

VI. Authorized Redisclosure

Data Recipient is authorized to redisclose UI Data (except UI Data stored in the ACISS system) without prior written authorization of DWD to a prosecuting agency or law enforcement agency if that agency needs the UI Data to pursue criminal charges or criminal investigations and a representative of that agency could subpoena the records from the DWD, even if no subpoena has actually been served. UI Data may also be redisclosed, when necessary in the opinion of the Data Recipient, for discovery or into the official records of a court proceeding or administrative hearing.

VII. Duties With Respect to Breach

A. Suspension of UI Data Sharing by DWD; Termination of Agreement by DWD for Cause; Directions Regarding UI Data; Audit.

If DWD believes that Data Recipient has failed to comply with any provision of this Agreement, DWD may suspend data sharing under this Agreement and decline to make further disclosure of UI Data until DWD is satisfied that sufficient corrective action has been taken and there will be no further failure. Whether or not there has been any prior suspension of this Agreement, DWD may at its option immediately terminate this Agreement if Data Recipient fails to make prompt and satisfactory action to correct a failure or breach of security or confidentiality with regard to UI Data it has received from DWD; or if Data Recipient otherwise breaches this Agreement; or if DWD considers itself insecure in the protection of UI Data disclosed to Data Recipient.

B. Mitigation of Breach of Security or Breach of Confidentiality.
In the event that Data Recipient becomes aware of a failure or breach by any of its employees or agents of security or confidentiality with regard to UI Data it has

DocuSign Envelope ID: 10489A29-B845-4741-AFAA-C34BB47D7AD0

received from DWD or in the event it has reason to suspect that such a failure or breach of security or confidentiality has occurred, including any unauthorized use, disclosure, public exposure or loss of or unauthorized access to UI Data, Data Recipient shall:

1. Within the same business day, notify DWD of the failure or breach, known and suspected, and supply to DWD all available information concerning the nature and extent of such failure or breach.

2. In consultation with DWD take immediate steps to mitigate any harmful effects of such failure or breach and to prevent any additional failure or breach.

3. Cooperate with DWD to obtain assistance of law enforcement, injunctive relief, or other judicial relief to prevent or curtail any threatened or actual breach of security of UI Data or redisclosure or unauthorized use of UI Data, and to recover UI Data from any person.

4. Take reasonable corrective action prescribed by DWD.

C. Mitigation of Exposure of Personally Identifiable Information.

Definition: As used in this Agreement, "Personally Identifiable Information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted or altered in any manner that renders the element unreadable: (a) the individual's Social Security number; (b) the individual's driver's license number or state identification number; (c) the individual's date of birth; (d) the number of the individual's financial account, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account; (e) the individual's DNA profile; or (f) the individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical characteristic.

If it is determined by DWD that the failure or breach has or likely resulted in the unauthorized use, access, disclosure, public exposure or loss of Personally Identifiable Information provided by DWD to Data Recipient, Data Recipient shall, at its own expense, take the following corrective actions that are directed by DWD:

1. Mitigate any harmful effect on individuals whose Personally Identifiable Information was used, accessed, disclosed, publicly exposed or lost.

2. Notify the affected individuals by mail or other method prescribed by DWD to communicate with individuals. If Data Recipient cannot with reasonable diligence determine the mailing address of certain affected individuals and DWD has not previously communicated with that

DocuSign Envelope ID: 10489A29-B845-4741-AFAA-C34BB47D7AD0

individual, Data Recipient shall provide notice by a method reasonably calculated to provide actual notice to such individuals.

3. Notify consumer reporting agencies of the unauthorized use, access, disclosure, public exposure or loss of Personally Identifiable Information.

4. Provide credit monitoring and identity theft insurance to affected individuals under the terms of a statewide data breach and credit monitoring services agreement that is in effect at the time that credit monitoring and identity theft insurance is provided.

D. Remedies for Breach of this Agreement.

To the extent permitted by law, Data Recipient shall be liable for and hold DWD harmless for all losses, costs, claims or damages sustained by DWD due to: (1) unauthorized use, access, disclosure, public exposure or loss of UI Data resulting from any failure or breach of security or confidentiality of UI Data maintained by Data Recipient or its agents under this Agreement, whether such failure or breach is initiated or caused by Data Recipient or its agents or by other persons or entities not party to this Agreement; or (2) other breach of this Agreement by Data Recipient or its agents.

VIII. Term and Termination of Agreement

This Agreement will be effective upon signature by both parties. Any party may terminate this Agreement without cause by giving written notice of such termination to the other party.

The duties of Data Recipient regarding security, confidentiality, maintenance and destruction of UI Data and duties with respect to breach (Sections V, VI, and VII) under this Agreement shall survive the termination of the Agreement. Following termination of this Agreement, Data Recipient shall adhere to DWD's written directions regarding maintenance, return and destruction of all UI Data and records of use and disclosure of UI Data.

IX. Agreement Compliance Monitoring

DWD will periodically monitor the Data Recipient's compliance with the terms and conditions of this Agreement.

DWD will send Data Recipients and its agents, if any, a compliance self-assessment packet once every three years. Data Recipient shall complete the compliance self-assessment questionnaire. DWD will review the compliance self-assessment questionnaire to ensure Data Recipients compliance with the terms and conditions of this Agreement. Data Recipient shall cooperate with DWD to clarify questionnaire responses and take corrective actions when DWD identifies areas of non-compliance.

DWD will send Data Recipient and its agents, if any, a compliance

DocuSign Envelope ID: 10489A29-B845-4741-AFAA-C34BB47D7AD0

acknowledgement packet on an annual basis, except during the years the Data Recipient supplies a compliance self-assessment questionnaire. Data Recipient shall sign and return the compliance acknowledgment form certifying their compliance with the terms and conditions of this Agreement.

X. Audit

DWD may elect to audit the compliance of Data Recipient and its agents with this Agreement with 30 days written notice before or within 30 days following termination of this Agreement. Audits may not exceed one time annually, unless the audit relates to a breach of the Agreement by Data Recipient or its agents. Audit requirements shall adhere to any applicable state and federal requirements. Audit scope, timing, access, and cost may be mutually amended in whole or in part by both Parties to be acceptable to both Parties. Data Recipient and its agents shall fully cooperate in the conduct of such an audit by DWD and its agents, including, if requested by DWD, scheduled on-site inspections. Such audit shall extend to matters of compliance by Data Recipient and its agents both before and after termination of the Agreement. In the event of an audit preceded by a breach of the Agreement by Data Recipient or its agents, reasonable costs incurred by DWD to conduct the audit, including DWD's expense of compensating retained auditors, shall be charged to and paid by Data Recipient.

XI. Authority to Request and to Provide Data

A. All inquiries and notices from DOJ that are required by this Agreement or that relate to this agreement, except for the actual requests for UI Data, are to be addressed to:

Jeff Becker
Internal Security Officer/UI Data Sharing Coordinator
Unemployment Insurance Division
201 E Washington
Ave PO Box 7974
Madison, WI 53707-7974
Email: UIDataSharingCoordinator@dwd.wisconsin.gov

B. All inquiries and notices from DWD required by this Agreement or involving this agreement, except for the actual response to supply UI Data, are to be addressed to:

Ryan Shogren
Director, Special Operations Bureau
Department of Justice, Division of Criminal Investigation
17 West Main Street
PO Box 7857
Madison, WI 53707
Email: shogrenrt@doj.state.wi.us

DocuSign Envelope ID: 10489A29-B845-4741-AFAA-C34BB47D7AD0

XII. Authority, Signing and Integration

A. DWD has granted full authority to sign this agreement

to: Mark Reihl
Division Administrator
Unemployment Insurance Division
201 E Washington Ave
PO Box 7905
Madison, WI 53707-7905
Mark.Reihl@dwd.wi.gov

B. Data Recipient has granted full authority to sign this Agreement to:

Eric Wilson
Deputy Attorney General
Department of Justice
17 W. Main St.
Madison, WI 53707

This Agreement may be signed in counterpart and amended only in writing signed by the parties.

AGREED:

Wisconsin Department of Workforce Development

DocuSigned by:
Mark Reihl
9D6AEA7D90DA430...

10/19/2021

Mark Reihl (Date)
Division Administrator
Unemployment Insurance Division

Wisconsin Department of Justice

8/3/2021

E (Date)
Deputy Attorney General